Storm протокола ARP устранения неполадок Nexus 7000 без внутриполосного перехвата

Содержание

Введение

Этот документ описывает, как устранить неполадки шторма ARP без любого внутриполосного трафика ARP.

Общие сведения

Шторм ARP является общей атакой атаки Denial of Service (DoS), которую вы видели бы в среде ЦОД.

Общий логик переключения для обработки пакета ARP то, что:

- Пакет ARP с широковещательным Destination Media Access Control (MAC)
- Пакет ARP с получателем MAC индивидуальной рассылки, который принадлежит коммутатору

если коммутируемый виртуальный интерфейс (SVI) будет подключен в Vlan получения, будет обработан процессом ARP в программном обеспечении.

Этой логикой, если существуют один или несколько хостов malicous, продолжают передавать запрос ARP в Vlan, где коммутатор является шлюзом того Vlan. Запрос ARP будет обработан в программном обеспечении, следовательно вызывает разбиваемый коммутатор. В некоторой более старой модели коммутатора Cisco и версии, вы будете видеть, что процесс ARP берет использование ЦПУ до высокого уровня, и система слишком занята для обработки другого трафика уровня управления. Обычный способ для отслеживания такой атаки должен выполнить внутриполосный перехват для определения адреса MAC источника шторма ARP.

В ЦОД, где Nexus 7000 действует как шлюз агрегации, такое влияние уменьшено CoPP на Коммутаторах Cisco Nexus серии 7000. Вы могли все еще выполнить внутриполосный перехват Ethanalyzer на руководстве по поиску и устранению проблем Nexus 7000 для определения адреса MAC источника шторма ARP, так как Контроль уровня управления (CoPP) является просто бандитом, замедляющимся, но не elminating шторм ARP, мчащийся к ЦП.

Как насчет этого сценария, где:

- SVI не работает

- Никакой чрезмерный пакет ARP, являющийся избыточным направлением к ЦП
- Никакая высокая загрузка CPU из-за процесса ARP

Коммутатор, однако, все еще видит связанную проблему ARP, например, прямой подключенный узел имеет неполный ARP. Это возможно вызвано штормом ARP?

Ответ - да на Nexus 7000.

Основная причина

В дизайне линейной платы nexus 7000, для поддержки процесса пакета ARP в CoPP запрос ARP будет вести специальный логический интерфейс (LIF) затем быть скоростью, ограниченной CoPP в механизме пересылки (FE). Это происходит независимо от того, у вас есть SVI для Vlan или нет.

Следовательно, в то время как заключительное решение по перенаправлению, сделанное FE, не должно передавать запрос ARP к внутриполосному ЦП (в случае никакой SVI для vlan), счетчик CoPP все еще обновлен. Это приводит к CoPP, насыщаемому с чрезмерным запросом ARP и отбрасыванием легитимного запроса ARP / ответ. В этом сценарии вы не будете видеть чрезмерных внутриполосных пакетов ARP, но все еще быть влияемым штормом ARP.

У нас есть расширенный дефект CSCub47533, поданный в течение этого дня CoPP одно поведение.

Решение

Могло быть несколько опций для определения источника ARP, влетают как ураган этот сценарий. Одна эффективная опция:

- Сначала определите, из какого модуля шторм ARP прибывает

```
N7K# sh policy-map interface control-plane class copp-system-p-class-normal
```

```
Control Plane
service-policy input copp-system-p-policy-strict

class-map copp-system-p-class-normal (match-any)
match access-group name copp-system-p-acl-mac-dot1x
match exception ip multicast directly-connected-sources
match exception ipv6 multicast directly-connected-sources
match protocol arp
set cos 1
police cir 680 kbps bc 250 ms
conform action: transmit
violate action: drop
module 3:
conformed 4820928 bytes,
5-min offered rate 0 bytes/sec
peak rate 104 bytes/sec at Thu Aug 25 08:12:12 2016
 violated 9730978848 bytes,
```

```
 5-min violate rate 6983650 bytes/sec
 peak rate 7632238 bytes/sec at Thu Aug 25 00:43:33 2016
module 4:
conformed 4379136 bytes,
5-min offered rate 0 bytes/sec
peak rate 38 bytes/sec at Wed Aug 24 07:12:09 2016
violated 0 bytes,
5-min violate rate 0 bytes/sec
peak rate 0 bytes/sec
...
```

- Второе использование Процедура ЭЛАМА для получения всего пакета ARP, поражающего модуль. Вы, возможно, должны были бы сделать это несколько раз. Но если существует штормовое продолжение, шанс, вы перехватываете нарушить пакет ARP, намного лучше, чем легитимный пакет ARP. Определите адрес MAC источника и Vlan от перехвата ЭЛАМА.